Use of Personal and Service Users Gadget Policy

PRN-142: Use of Personal and Service Users Gadget Policy
Company Name: AI Auto-Tech Ltd
Trading/Business Name: Trusted Companionship
Company Registration Number: 15556946
SIC Code: 88100 – Social Work Activities Without Accommodation for the Elderly and Disabled
Email: info@trustedcompanionship.com
Version Number: V01 20260815
Date of Review: (August 2026)

---

1. Policy Introduction

Trusted Companionship, the trading name of AI Auto-Tech Ltd, is committed to ensuring safe, lawful, and appropriate use of **personal gadgets** (phones, tablets, laptops, smart devices) and **service users' gadgets** during companionship sessions. This policy protects:

- Service user privacy
- Organisational data
- Safeguarding requirements
- Cyber-security integrity
- Professional boundaries

Companions must follow strict rules when using any digital device in the presence of service users.

2. Key Principles

- **Safety:** Gadget use must never compromise safeguarding.
- **Privacy:** Service user information must remain confidential at all times.
- **Professionalism:** Gadget use must support companionship, not distract from it.
- **Boundaries:** Personal gadgets must not be used for personal communication during sessions.
- **Cyber-security:** Devices must comply with PRN-111 and PRN-112.
- **Non-duplication:** Gadgets must not be used to perform tasks already provided by external professionals.
- **Consent:** Service user gadgets must never be used without explicit permission.

3. Policy Statement

Trusted Companionship ensures that:

- Staff use personal gadgets responsibly and professionally
- Service user gadgets are handled safely and lawfully
- No service user data is stored on personal devices
- Gadget use aligns with safeguarding and GDPR requirements
- Digital boundaries are maintained at all times
- Cyber-security protocols are followed
- Gadget misuse is treated as a safeguarding and disciplinary breach

4. Purpose

- Protect service user privacy and data
- Maintain professional boundaries
- Prevent cyber-security risks
- Ensure lawful and ethical gadget use
- Provide clear guidance for staff
- Strengthen safeguarding and risk management

5. Scope

This policy applies to:

- All employees
- Volunteers
- Contractors
- Agency workers
- Zero-contract workers (**PRN-149**)

It covers:

- Personal gadgets
- Service user gadgets
- Digital communication
- Data storage

- Cyber-security
- Safeguarding
- Documentation

6. Related Policies

PRN-111 Cyber Security Policy PRN-112 Data Protection and GDPR Policy PRN-102 Compliance Monitoring PRN-109 Companionship Standards Policy PRN-143 Wellbeing Monitoring Policy PRN-145 Working in Pairs and Multi-Staff Working Policy PRN-147 Proxy Working Principle PRN-150 Working with Vulnerable Children Policy

7. Rules for Using Personal Gadgets

7.1 Permitted Use

Personal gadgets may be used for:

- Accessing authorised work systems
- Contacting management
- Reporting safeguarding concerns
- Documenting sessions (via authorised platforms only)

7.2 Prohibited Use

Personal gadgets must **not** be used for:

- Personal calls or messages during sessions
- Social media browsing
- Taking photos or videos of service users
- Storing service user information
- Using personal email for work
- Connecting to service user Wi-Fi networks
- Playing personal music or videos
- Sharing personal contact details
- Proxy working
- Shift swapping without TC approval

8. Rules for Using Service Users' Gadgets

8.1 Permitted Use

Service user gadgets may be used **only when**:

- The service user requests assistance
- The task is safe, appropriate, and non-clinical
- The task does not involve accessing sensitive information
- The companion has explicit permission

Examples include:

- Helping a service user make a call
- Helping a service user play music
- Helping a service user access entertainment
- Helping a service user navigate simple apps

8.2 Prohibited Use

Companions must **never**:

- Access service user emails
- Access service user banking apps
- Access service user social media
- Access service user private messages
- Store organisational data on service user devices
- Connect personal devices to service user gadgets
- Transfer files between devices
- Use service user gadgets for companionship documentation
- Use service user gadgets to contact external professionals
- Use service user gadgets to manage care or clinical tasks

9. Safeguarding Requirements

Gadget use must never compromise safeguarding.

Companions must:

- Avoid digital contact with children
- Avoid sharing personal contact details
- Follow gender-based allocation rules

- Report digital safeguarding concerns immediately
- Document digital risks accurately

If external professionals already provide digital support:

- Companions must skip that service
- Document: *"Service already being provided by other service: {name of service}."*
- Avoid duplication
- Escalate concerns to management

10. Cyber-Security Requirements

Companions must:

- Follow PRN-111 Cyber Security Policy
- Use strong passwords
- Avoid public Wi-Fi
- Avoid suspicious links
- Avoid unauthorised apps
- Keep devices updated
- Lock devices when unattended
- Never disable security settings

Unauthorised access is a disciplinary and safeguarding breach.

11. Data Protection Requirements

Companions must:

- Follow PRN-112 Data Protection and GDPR Policy
- Never store service user data on personal devices
- Never share data through personal messaging apps
- Never send data via personal email
- Never screenshot service user information
- Never photograph service users
- Use only authorised organisational systems

12. Documentation Requirements

Companions must document:

- Gadget-related safeguarding concerns
- Digital risks
- External professionals present
- Multi-staff involvement
- “Service already being provided” entries

Records must be factual, objective, and securely stored.

13. Prohibited Conduct

Companions must **not**:

- Use gadgets for personal entertainment
- Use gadgets to avoid engagement
- Allow service users to access personal devices
- Share personal contact details
- Engage in proxy working
- Swap shifts without TC approval
- Use gadgets to communicate privately with service users
- Use gadgets to bypass organisational systems

14. Roles and Responsibilities

14.1 Trustees

- Oversee governance and compliance

14.2 Senior Management

- Ensure safe digital practice
- Approve policy changes

14.3 DSL

- Review digital safeguarding concerns
- Provide guidance and training

14.4 Managers

- Support staff

- Conduct digital risk assessments
- Review documentation

14.5 Staff

- Follow standards
- Maintain boundaries
- Report concerns
- Document accurately

15. Non-Compliance

Non-compliance may include:

- Data breaches
- Unsafe digital behaviour
- Boundary breaches
- Safeguarding failures
- Proxy working
- Poor documentation

Consequences may include:

- Retraining
- Formal warnings
- Suspension
- Termination
- Referral to safeguarding authorities
- Legal action

16. Policy Review

This policy will be reviewed annually or sooner if required due to:

- Legislative changes
- Cyber-security developments
- Organisational changes
- Audit findings